Secure Supply Chain Enablement using JTAG IEEE 1149.1™ | ECID and Non-Volatile Memory

Sidense

ABSTRACT

The Internet of Things (IoT) and automotive markets are predicted to be major drivers of the semiconductor industry over the next 5-10 years. Both of these markets, with their widespread interconnectivity and often mission-critical operations, require effective and efficient ways to manage SoC security throughout their product design, manufacturing and life cycles.

IoT, often considered the next major driver for the semiconductor industry (after the smartphone) is not one application but several, addressing multiple markets, often with diverse requirements. The number of units shipped, for any one chip type, is split over several market segments, each often requiring different performance and/or features. In a similar fashion, automotive ICs need a range of capabilities to cover the wide variety of vehicles in which they will be used.

In order to maximize ROI and to minimize the number of unique chips, semiconductor vendors addressing the IoT and automotive spaces (among others) are turning to a platform concept in which multiple markets may be addressed by a single chip. Chip features may be enabled or disabled during manufacture or in the field. While chip cost is fixed, the chip selling price may be set according to the features enabled and markets being addressed. While not a particularly new concept, the diversity and price sensitivity of these markets are important considerations.

Any IC solution has to be cost-effective and implemented in a secure manner that minimizes the chance of counterfeiting and misappropriation of features – this, in essence, is Secure Supply Chain Enablement. While features to assure security are normally part of a chip's design, it is sometimes not adequately taken into account during manufacture. Key features of a Secure Supply Chain Enablement scheme are the ability to store, at time of manufacture, data such as wafer mapping and chip grading information such as speed and temperature. The authentication data, along with a unique chip ID, then needs to be publicly and cheaply accessible throughout the chip's lifetime, while simultaneously providing a reliable way for the SoC vendor to access and update secure capabilities such as in-the-field feature enablement.

This paper presents a Non-Volatile Memory (NVM) subsystem that may be used in an Arm Cortex M5-based SoC for cost-sensitive and low-power IoT, automotive and other applications. It comprises a one-time programmable (OTP) memory that may be used in an emulated multi-time programmable (eMTP) mode. The memory array seamlessly interfaces to on-chip resources via the Advanced Peripheral Bus (APB) and the JTAG IEEE 1149.1™-2013 user defined Electronic Chip ID (ECID) register to access authentication data within the chip's supply chain. When implemented in processes such as TSMC's 28HPC+, 40ULP or 16FFC, the NVM subsystem provides key manufacturing and tracking data for chip authentication and in-field feature enablement.

Secure Supply Chain Enablement using JTAG IEEE 1149.1™| ECID and Non-Volatile Memory

TSMC NA OIP Ecosystem Forum

September 13, 2017

Andrew Faulkner, Sidense; Senior Director, Product Management
Craig Downing, Sidense; Product Line Manager
CJ Clark, Intellitech; CEO and President | IEEE 1149.1-2013 Working Group Chair

1

About Sidense Corp | Your Trusted Memory Partner

- Well Established → Headquarters in Ottawa Canada → Privately Owned
- Well Funded → Stable long-term investors → 4 Year Revenue 32% CAGR
- Well Resourced → 70+ Employees → Global Support Centers

Leading supplier of Non-Volatile, One-Time Programmable (OTP) memory IP, in standard-logic CMOS processes with no additional masks or process steps

2

Sidense | By the Numbers

- ~170 Engaged Customers
- ~670 Licenses
- ~170 Patents (Filed and pending)
- ~9 ~30 Fabs at multiple foundries
- ~19 ~60 Processes

Sidense's market-leading technology is validated by design wins with multiple Tier-1 customers and foundries, used in multiple advanced nodes and processes, and secured with IP patents granted in multiple jurisdictions

3

About Intellitech Corporation | IEEE 1149.x Solutions

Leading supplier of IEEE 1149.1-2013 based ATE & Silicon Instruments

- Well Established → Headquarters in Dover, NH → Privately Owned
- Stable → Stable long-term investors → 29 Years 100s of customers
- ECID Expertise → ECID implemented in all Intellitech IC → Proven

4

About Intellitech Corporation | IEEE 1149.x Solutions

5

Semiconductor Supplier Pain Points

ROI difficult to achieve	Many Smart Connected applications like IoT, automotive, industrial and medical are lower volume and diverse
In-field Support Costs	In-field patches, provisioning, recalls, truck-rolls, "out of service"
Increased security vulnerability	Many Smart Connected applications are "low cost" nodes where complex security strategies are NOT affordable
Counterfeiting	An increasing concern, leading to loss of revenue and safety concerns

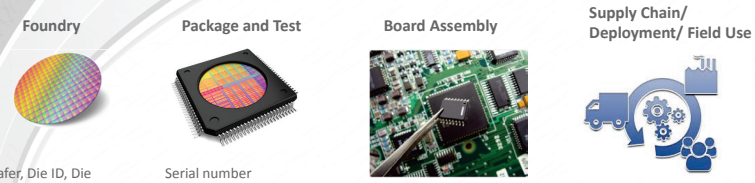
6

ECID and Supply Chain Enablement

ROI difficult to achieve	Platform concept and ECID allows increased flexibility in product SKUs
In-field Support Costs	Ability to securely apply in-field patches, upgrades and feature provisioning
Increased security vulnerability	Level of security appropriate to market being addressed
Counterfeiting	"In birth" ECID of IP/IC mitigates chance of counterfeiting

7

Anti-Cloning ECID and Tracking | Throughout the Supply Chain



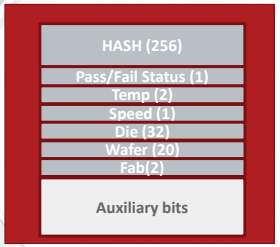
Foundry	Package and Test	Board Assembly	Supply Chain/ Deployment/ Field Use
Wafer, Die ID, Die location and grading	Serial number Tracking Code Hash/Encrypted unique ID Logging IC data on a central database Device feature enablement/ customization	Authentication Verifying IC data from a central database Tracking information System codes/keys	Authentication Inventory control Device tracking Feature enablement/ revocation

ECID = Electronic Chip IDs

8

IEEE 1149.1™-2013 | Enabling IC Counterfeit Protection

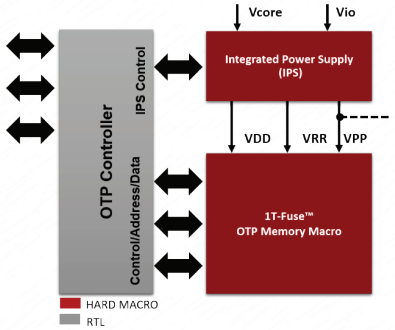
- ECID - Electronic Chip ID as part of the standard
- Also Available via IEEE 1149.10-2017



- Enables tracking of dice from wafer to field.
- Records die position on wafer with unique ID
- Records test results, temperature and speed grade.
- Anti-cloning security: Prevent cloned chips being sold or used
  - Provide IEEE 1149.1-2013 standard access to ECID for authentication.
- Prevent fraudulent IC package remarking
  - Identify falsely marked parts (e.g., commercial parts remarked as military or industrial).

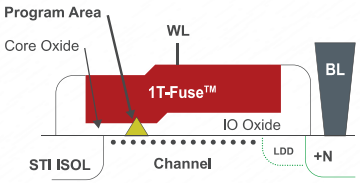
1T-NVM | A System-Level solution

- OTP Memory Macro
  - Sidense 1T-Fuse™ bit cells
  - Small footprint
  - Wide range of configurations from low to high densities
  - Physically Secure
- Power Supply Options
  - Integrated Power Supply (IPS)
  - Options for different power supply scenarios and use cases
  - Charge pump for programming
- Controller
  - Controls programming and test of OTP memory
  - Supports Test, ECID and eMTP
  - Additional security features



1T-Fuse™ | Split Channel Bit-Cell

- Reliably programmed through a controlled, non-reversible oxide breakdown
- Standard CMOS process
- Widespread industry adoption
- Proven silicon across all nodes from 180nm to 16nmFF for a range of TSMC's standard logic and specialty processes (BCD, HV, CIS, ULP, RF)



Planar Implementation

1T-NVM bit cell | Inherently Physically Secure

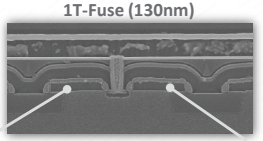
- Programming through permanent structural change in few atomic layers (far from diffusion)
- No isolated diffusion nodes exposed for attack
- No physical attack can reveal programmed state in FinFET or HKMG
- No leakage in non-programmed state
- State cannot be changed through exposure to high temperature, voltage or radiation
- No charge or voltage involved in state retention (unlike floating gate NVM, e.g. flash)
- State (even for a few bits) is virtually impossible to detect using physical attack or reverse engineering techniques

Typical eFuse

Non-Programmed Programmed

William Tonti "eFuse Design and Reliability"

1T-Fuse (130nm)



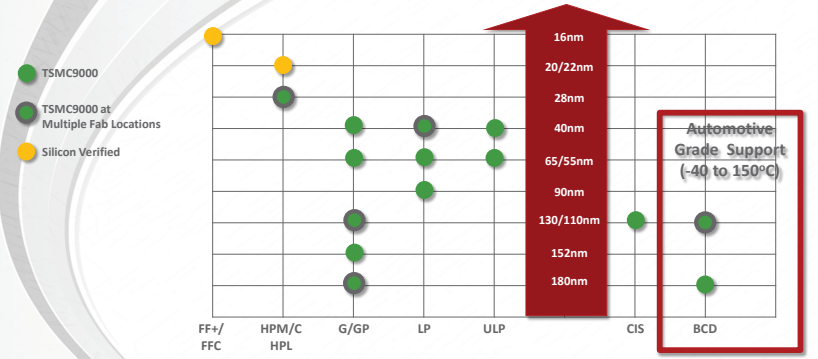
Non-Programmed Programmed

Tamper Resistance | By Design

- Built-in redundant and/or differential mode
  - Highest read margins at wide operating voltage and temperature range
  - Prevents tampering using ambient conditions
- Built-in read timer
  - Prevents tampering with clock speed or access cycle
- Built-in hidden ROM / test OTP address space
- Built-in temperature compensation in IPS
  - Read voltage automatically adjusted to detect junction temperature – prevents any form of attack through high/low temperature exposure
- No shift registers
  - No stored data
- Delayering protection techniques
  - Routing to disable access with partial metal removal

13

Sidense 1T-NVM |TSMC Process Coverage



14

1T-NVM Flexibility | ECID and Generic NVM Use

- Top 1024 bits used for ECID and die information storage
- In this example the remaining 64Kbits used for other NVM uses
  - Boot Code
  - Configuration Settings
  - Security Keys

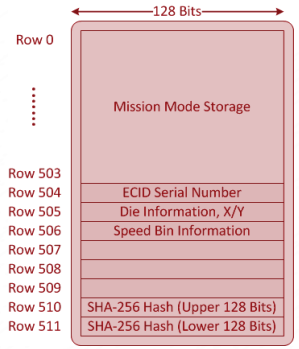
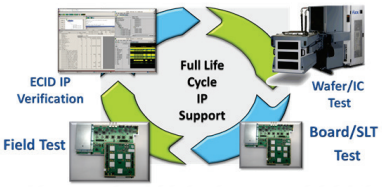


Image © 2017 Intellitech

15

IEEE 1149.1-2013 ECID | Intellitech and Sidense 1T-NVM

- Turnkey solution from Intellitech with Sidense 1T-NVM
  - IEEE 1149.1 JTAG write/read instrument with integrated controller
    - Private/Secure write/programming
    - Public non-secure read of ECID
  - IEEE 1149.1-2013 compliant Electronic Chip ID read access
  - Write/read shared interface for use with mission-mode logic or CPU
  - Pre-verified ECID Instrument IEEE 1149.1-2013 package description
  - Pre-verified IEEE 1149.1-2013 PDL (Procedural Description Language) files.
  - Proven, patented, on-chip memory programming via US Patent #6,594,802 and foreign counterparts.

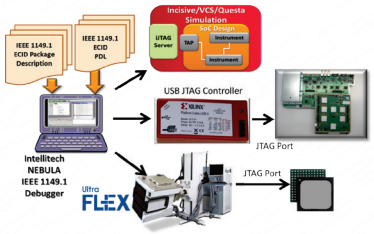


Electronic Chip IDs (ECIDs) are unique values which allow a die to be tracked through its entire life cycle. An ECID can be used for correlation of failures in SLT (System Level Test) and in the field back to test escapes in the production ATE environment.. When coupled with standard security measures, the ECID can also be used for anti-cloning of an integrated circuit.

16

IEEE 1149.1-2013 ECID | Intellitech and Sidense 1T-NVM

- Intellitech NEBULA software
  - Allows users to write, read, and lock the Sidense 1T-NVM with PDL scripts in:
    - Simulation environments
    - Verification environments
    - System and board level IC test
    - Production ATE
  - PDL and 1149.1-2013 compliant package file can be reused across multiple IC devices
  - Low-cost read-only version for public authentication of ECID
  - IEEE 1149.1 or IEEE 1149.10 (Serial Peripheral Interface - SPI) protocol

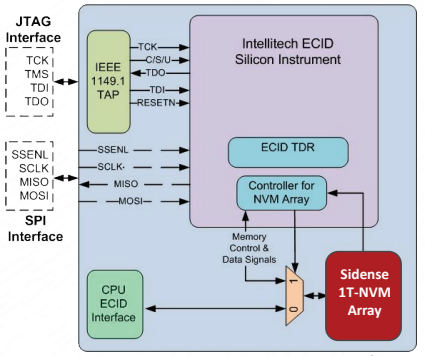


Platform for working with 1T-NVM based ECID

(UltraFlex photo courtesy of Teradyne and used with permission)

IEEE 1149.1-2013 ECID | Intellitech and Sidense 1T-NVM

- Intellitech ECID Silicon Instrument
  - IEEE 1149.1-2013 package with Procedural Description Language (PDL) for programming
    - Supports ECID reading and private programming of the ECID
    - Supports industry-standard IEEE 1149.1-2013 JTAG/IJTAG tools
    - Supports SPI via IEEE 1149.10-2017 descriptions
    - Plug-in for verification engines
    - Plug-in for validation on ATEs
    - Provides test pattern generation for ATE
    - Provides board and system level access to ECID
- Sidense 1T-NVM for ECID storage
  - Highly secure and robust permanent ECID storage
  - Broad range of TSMC processes supported
  - 1T-NVM for ECID available for 180nm to 16nm in TSMC's standard logic and specialty processes (BCD, HV, CIS, ULP, RF)



CPU, IEEE 1149.1, or SPI protocol

Image © 2017 Intellitech

Summary

- IEEE 1149.1™-2013 ECID Provides a standards-based solution for tracking devices and anti-cloning protection for the IC supply chain
- Intellitech with Sidense 1T-NVM provides a turnkey, secure, robust ECID solution
- Highly secure and robust permanent ECID storage
- Broad range of TSMC processes supported from 16nm to 180nm including specialty processes